

WHAT IS CLAIMED IS:

- 1 1. A method of integrating telephony function with security and guidance features
2 on an Internet appliance comprising the steps of:
 - 3 selecting a communication access number using a selection means, said
4 communication access number operable to access a communication link via said
5 Internet appliance;
 - 6 alerting a user of said Internet appliance when an attempt is made to select said said
7 communication link via a dialing action of said Internet appliance using said
8 communication access number; and
 - 9 receiving an authorization for said dialing action by said user of said Internet
10 appliance.
- 1 2. The method of claim 1 wherein said authorization comprises the sub steps of:
 - 2 prompting said user to enter a user personal identification means (PIM) in
3 response to selecting said communication access number;
 - 4 initiating a pre-determined security protocol to retrieve a corresponding secure
5 PIM for comparison;
 - 6 correlating said user personal identification means with said secure PIM;
7 authorizing or rejecting said dialing action in response to said correlation;
 - 8 retrieving secure device driver code for executing said dialing action using said
9 security protocol in response to said authorization;
 - 10 displaying, if said dialing action is authorized, a connectivity cost alert for said
11 communication link; and

12 executing said dialing action using said device driver code for said
13 communication link in response to said authorization and a user response to said
14 connectivity cost alert.

- 1 3. The method of claim 1, further comprising the step of:
2 using said security protocol for encrypting and decrypting information
3 transmitted on said communication link in response to authorizing said dialing action
4 for said communication link.
- 1 4. The method of claim 1, wherein said security protocol is a Public/Private key
2 encryption protocol.
- 1 5. The method of claim 1, wherein said PIM is used to grant or block access to
2 certain area or country telephony codes.
- 1 6. The method of claim 1, further comprising the step of:
2 matching said communication access number with an actual system entered
3 communication access number.
- 1 7. The method of claim 1, further comprising the steps of:
2 monitoring an incoming call for a caller ID; and
3 answering and routing said incoming call to a receiving device on the basis of
4 said incoming telephone number.

- 1 8. The method of claim 1, further comprising the step of:
2 using a built-in key escrow function to notify a trusted server of a current
3 dynamic host configuration protocol (DHCP) assigned IP address along with a key
4 indicating authenticity of transmission so that voice over IP services between devices
5 and a web page server lookup may be performed in a DHCP environment without
6 side-channel communication for call or web reference look-up.
- 1 9. The method of claim 1, wherein activating said selected communication access
2 number comprises selecting said communication access number from a displayed
3 Internet web page hot spot.
- 1 10. The method of claim 1, wherein said communication access number is selected
2 using an actual or virtual keypad of said Internet appliance.
- 1 11. The method of claim 1, wherein said communication link comprises
2 a non-concurrent shared dial-up public switched telephone network (PSTN)
3 connection between a telephone connection and an Internet connection.
- 1 12. The method of claim 1, wherein said communication link has separate
2 connections for an Internet connection and a telephone connection.
- 1 13. The method of claim 1, wherein said communication link comprises a
2 concurrent communication link for an Internet and a telephone connection.

1 14. A system for integrating telephony function with security and guidance features
2 on an Internet appliance (IA):

3 one or more personal identification means (PIM) input units coupled to a
4 system bus in said ICA, said PIM input units operable to generate unique PIM signals;

5 a security protocol circuit operable to encrypt, decrypt, store and retrieve said
6 PIM signals and device driver code;

7 a PIM verification circuit operable to receive said PIM signals and compare
8 them to secure predetermined PIM signals, said PIM verification circuit generating a
9 verification signal;

10 one or more Modems coupled to a dialing action controller and to
11 communication lines; said Modems operable to send and receive communication data;
12 and

13 a dialing action controller (DAC) coupled to said system bus and said Modems,
14 said DAC operable receive a dialing action request and to alert a user of said dialing
15 action and to enable or disable said dialing action to said Modems in response to said
16 verification signal and a user signal.

1 15. The system of claim 13, wherein said authorization unit comprises:

2 a smart card reader;

3 a biometric input unit;

4 a personal identification number input unit; and

5 a voice recognition input unit,

1 16. The system of claim 13, wherein said Modem comprises:

2 a digital subscriber line (DSL) Modem;

- 1 17. The system of claim 13, wherein said Modem comprises:
2 a wireless cellular modem;
- 1 18. The system of claim 13, wherein said Modem comprises:
2 a wireless personal communication system (PCS) modem;
- 1 19. The system of claim 13, wherein said Modem comprises:
2 a cable Modem.
- 1 20. The system of claim 13, wherein said Modem comprises a public subscriber
2 telephone network (PSTN) Modem.
- 1 21. The system of claim 13, wherein said DAC alerts said user of a dialing action
2 by display on a user display screen coupled to said IA.
- 1 22. The system of claim 13, wherein said DAC retrieves a connectivity cost and
2 alerts said user of a connectivity cost associated with a requested dialing action if said
3 dialing action is authorized.
- 1 23. The system of claim 13, wherein said user signal is a response by said user to
2 said connectivity cost alert for said dialing action.
- 1 24. The system of claim 13, wherein said user is given an option of communicating
2 on an established communication link in response to an authorized and enabled dialing
3 action using said security protocol.

1 25. The system of claim 13, wherein said DAC uses a built-in key escrow function
2 to notify a trusted server of a current dynamic host configuration protocol (DHCP)
3 assigned IP address along with a key indicating authenticity of transmission so that
4 voice over IP services between devices and a web page server lookup may be
5 performed in a DHCP environment without side-channel communication for call or
6 web reference look-up.

1 26. The system of claim 13, wherein said dialing action request comprises:
2 entering a communication access number via a keyboard keypad, a virtual
3 display keypad, or by clicking a "hot spot" on a Web page.

1 27. The system of claim 13, wherein said connectivity cost alert notifies a user of
2 an actual toll call cost for a communication link corresponding to said authorized and
3 enabled dialing action.

1 28. The system of claim 13, wherein said user is alerted of said dialing action
2 whether said dialing action was initiated locally or remote by another user.

1 29. The system of claim 13, wherein DAC monitors incoming communication
2 access numbers and directs communication to a answering or recording device or
3 forwards the communication to another communication link in response to comparing
4 said incoming communication access numbers to a predetermined, stored
5 communication access numbers list.

1 30. An Internet appliance, comprising:
2 a central processing unit (CPU);
3 a read only memory (ROM);
4 a random access memory (RAM);
5 a user interface adapter coupled to a keyboard and a mouse;
6 a display interface adapter coupled to a user display;
7 an I/O interface adapter;
8 a system bus;
9 a communication adapter; and
10 a security processor unit,
11 said security processor unit further comprising:
12 one or more personal identification means (PIM) input units coupled to
13 a system bus in said ICA, said PIM input units operable to generate
14 unique PIM signals;
15 a security protocol circuit operable to encrypt, decrypt, store and
16 retrieve said PIM signals and device driver code;
17 a PIM verification circuit, said PIM verification circuit operable to
18 receive said PIM signals and compare them to secure predetermined
19 PIM signals, said PIM verification circuit generating a verification
20 signal;
21 one or more Modems coupled to a dialing action controller and to
22 communication lines, said Modems operable to send and receive
23 communication data; and
24 a dialing action controller (DAC) coupled to said system bus and said
25 Modems, said DAC operable receive a dialing action request and to
26 alert a user of said dialing action and to enable or disable said dialing

action to said Modems in response to said verification signal and a user signal.

- 1 31. The Internet appliance of claim 29, wherein said PIM input unit comprises:
2 a smart card reader;
3 a biometric input unit;
4 a personal identification number input unit; and
5 a voice recognition input unit

 - 1 32. The Internet appliance of claim 29, wherein said Modem comprises:
2 a digital subscriber line (DSL) Modem.

 - 1 33. The Internet appliance of claim 29, wherein said Modem comprises:
2 a wireless cellular modem.

 - 1 34. The Internet appliance of claim 29, wherein said Modem comprises:
2 a wireless personal communication system (PCS) modem.

 - 1 35. The Internet appliance of claim 29, wherein said Modem comprises
2 a cable Modem.

 - 1 36. The Internet appliance of claim 29, wherein said Modem comprises a public
2 subscriber telephone network (PSTN) Modem.

 - 1 37. The Internet appliance of claim 29, wherein said DAC alerts said user of a
2 dialing action by display on a user display screen coupled to said IA.

1 38. The Internet appliance of claim 29, wherein said DAC retrieves a connectivity
2 cost and alerts said user of a connectivity cost associated with a requested dialing
3 action if said dialing action is authorized.

1 39. The Internet appliance of claim 29, wherein said user signal is a response by
2 said user to said connectivity cost alert for said dialing action.

1 40. The Internet appliance of claim 29, wherein said user is given an option of
2 communicating on an established communication link in response to an authorized and
3 enabled dialing action using data encryption.

1 41. The Internet appliance of claim 29, wherein said DAC uses a built-in key
2 escrow function to notify a trusted server of a current dynamic host configuration
3 protocol (DHCP) assigned IP address along with a key indicating authenticity of
4 transmission so that voice over IP services between devices and a web page server
5 lookup may be performed in a DHCP environment without side-channel
6 communication for call or web reference look-up.

1 42. The Internet appliance of claim 29, wherein said dialing action request
2 comprises:

3 entering a communication access number via a keyboard keypad, a virtual
4 display keypad, or by clicking a "hot spot" on a Web page.

1 43. The Internet appliance of claim 29, wherein said connectivity cost alert notifies
2 a user of an actual toll call cost for a communication link corresponding to said
3 authorized and enabled dialing action.

1 44. The Internet appliance of claim 29, wherein said user is alerted of said dialing
2 action whether said dialing action was initiated locally or remote by another user.

1 45. The Internet appliance of claim 29, wherein DAC monitors incoming
2 communication access numbers and directs communication to a answering or
3 recording device or forwards the communication to another communication link in
4 response to comparing said incoming communication access numbers to a
5 predetermined, stored communication access numbers list.

PRINTED IN U.S.A. 05/25/00